System and Methods for a Vernam Cipher, a Keyed One-Way Hash
and a Non-Cyclic Pseudo-Random Number Generator

Abstract:

5

The invention discloses a cryptographic system and consisting of three methods: a cryptographic Vernam stream cipher that permits software programs on separate computers to encrypt and decrypt information; a cryptographic keyed one-way hash that ensures the integrity and authenticity of a message; a non-cyclic

10   pseudo-random number generator that permits a software program inside a computer to create large amounts of pseudo-random bits at high data rates.